

1 In the claims:

2 1. A method for encrypting electronic books, comprising:
3 supplying an electronic book to be encrypted;
4 supplying an encryption key;
5 encrypting the electronic book using the encryption key;
6 supplying the encrypted electronic book;
7 supplying a decryption key; and
8 decrypting the encrypted electronic book using the decryption key.

9 2. The method of claim 1, wherein the encryption key and the decryption key are a
10 symmetric key.

11 3. The method of claim 2, further comprising generating the symmetric key.

12 4. The method of claim 3, wherein the symmetric key is generated randomly.

13 5. The method of claim 3, wherein the symmetric key is generated using a key
14 generator.

15 6. The method of claim 2, further comprising retrieving the symmetric key from a
16 key storage memory.

17 7. The method of claim 2, wherein the symmetric key is a transaction symmetric key,
18 the transaction symmetric key supplied by a certificate authority.

19 8. The method of claim 7, further comprising:
20 sending a transaction symmetric key request to the certificate authority;

1 encrypting the transaction symmetric key using a first party symmetric key to
2 produce a first encrypted transaction symmetric key;
3 delivering the first encrypted transaction symmetric key to a first party;
4 decrypting the first encrypted transaction symmetric key, wherein the electronic
5 book is encrypted by the first party using the transaction symmetric key;
6 encrypting the transaction symmetric key using a second party symmetric key to
7 produce a second encrypted transaction symmetric key;
8 delivering the second encrypted transaction symmetric key to a second party; and
9 decrypting the second encrypted transaction symmetric key, wherein the electronic
10 book is decrypted using the transaction symmetric key.

11 9. The method of claim 2, wherein the electronic book content and a transaction
12 symmetric key are encrypted by a first party and wherein the encrypted electronic book
13 content is supplied to a second party and the encrypted transaction symmetric key is
14 supplied to a third party.

15 10. The method of claim 9, wherein the second party requests the encrypted
16 transaction symmetric key from the third party.

17 11. The method of claim 10, wherein the third party decrypts the encrypted
18 transaction symmetric key using a first party symmetric key.

19 12. The method of claim 11, further comprising:
20 encrypting the decrypted transaction symmetric key using a second party
21 symmetric key;
22 supplying the encrypted transaction key to the second party; and
23 decrypting the encrypted transaction symmetric key using the second party
24 symmetric key.

1 13. The method of claim 12, further comprising completing a financial transaction
2 between the first party and the second party before supplying the encrypted electronic
3 book.

4 14. The method of claim 12, wherein the first party is an electronic book publisher,
5 the second party is an operations center of an electronic book distribution system and the
6 third party is a certificate authority.

7 15. The method of claim 12, wherein the first party is an electronic book distributor,
8 the second party is an electronic book viewer and the third party is a certificate authority.

9 16. The method of claim 2, further comprising:
10 encrypting the symmetric key with a private key and a private key encryption
11 process;
12 packaging the encrypted symmetric key and the encrypted electronic book; and
13 delivering the package to an electronic book viewer.

14 17. The method of claim 16, further comprising:
15 decrypting the encrypted symmetric key using a public key and a public key
16 decryption process; and
17 decrypting the encrypted electronic book using the decrypted symmetric key.

18 18. The method of claim 17, wherein the encryption method is one of a Merkle-
19 Hellman Knapsack technique, a RSA technique, a Pohlig-Hellman technique and a
20 Schnorr Signature technique.

21 19. The method of claim 2, wherein the symmetric key is a transaction symmetric key,
22 further comprising:

1 generating the transaction symmetric key at a first party location;
2 encrypting the electronic book using the transaction symmetric key and a
3 symmetric key encryption process;
4 delivering the encrypted electronic book to a second party;
5 encrypting the transaction symmetric key using a first shared symmetric key and
6 a first symmetric key encryption process;
7 delivering the encrypted transaction key to a third party;
8 decrypting the encrypted transaction symmetric key using the first shared
9 symmetric key and a first symmetric key decryption process;
10 requesting the decrypted transaction symmetric key from the third party;
11 encrypting the transaction symmetric key using a second shared symmetric key
12 and a second symmetric key encryption process;
13 delivering the encrypted transaction symmetric key to the third party;
14 decrypting the encrypted transaction symmetric key using the second shared
15 symmetric key and a second symmetric key decryption process; and
16 decrypting the delivered electronic book using the decrypted transaction
17 symmetric key.

18 20. The method of claim 19, further comprising completing a financial transaction
19 between the first party and the second party prior to delivery of the encrypted electronic
20 book.

21 21. The method of claim 19, further comprising completing a financial transaction
22 between the first party and the second party prior to delivery of the encrypted transaction
23 symmetric key to the second party.

24 22. The method of claim 2, wherein the symmetric key is a shared transaction
25 symmetric key, further comprising negotiating the shared transaction symmetric key

1 between a first party and a second party, wherein the first party supplies the encrypted
2 electronic book to the second party.

3 23. The method of claim 22, wherein the shared transaction symmetric key is
4 generated by first party and second party key negotiation algorithms.

5 24. The method of claim 22, further comprising:
6 encrypting the electronic book using the shared transaction symmetric key;
7 delivering the encrypted electronic book to the second party; and
8 decrypting the encrypted electronic book using the shared transaction symmetric
9 key.

10
11 25. The method of claim 2, further comprising:
12 supplying the encrypted electronic book using a first communications path; and
13 supplying the symmetric key using a second communications path.

14 26. The method of claim 2, further comprising supplying the encrypted electronic
15 book and the symmetric key using a same communications path.

16 27. The method of claim 26, wherein the encrypted electronic book and the symmetric
17 key are supplied simultaneously.

18 28. The method of claim 1, wherein the encryption key is generated by a first seed key
19 generation algorithm and the decryption key is generated by a second seed key generation
20 algorithm.

21 29. The method of claim 28, wherein the first and the second key generation
22 algorithms generate a seed key.

1 30. The method of claim 29, further comprising:
2 using the seed key at a first party location to generate a first shared transaction
3 symmetric key in a sequence of keys;
4 encrypting the electronic book using the first shared transaction symmetric key;
5 delivering the encrypted electronic book to a second party;
6 using the seed key at a second party location to generate a shared transaction
7 symmetric key corresponding to the first shared transaction symmetric key generated at
8 the first party location;
9 decrypting the encrypted electronic book using the shared transaction symmetric
10 key; and
11 repeating the process to generate a second and subsequent shared transaction keys
12 to encrypt and decrypt subsequent electronic books.

13 31. The method of claim 1, wherein the encryption key and the decryption key are
14 asymmetric.

15 32. The method of claim 31, wherein the electronic book is encrypted using one of
16 a Merkle-Hellman Knapsack technique, a RSA technique, a Pohlig-Hellman technique
17 and a Schnorr Signatures technique.

18 33. The method of claim 31, wherein the encryption key is a public key and the
19 decryption key is a private key.

20 34. The method of claim 31, wherein the encryption key is a private key and the
21 decryption key is a public key.

1 35. The method of claim 1, further comprising providing the decryption key with the
2 encrypted electronic book.

3 36. The method of claim 35, further comprising encrypting the decryption key.

4 37. The method of claim 1, further comprising using a first cryptographic algorithm
5 with the encryption key to encrypt the electronic book.

6 38. The method of claim 37, wherein the first cryptographic algorithm is one of DES,
7 PKZIP and BLOWFISH.

8 39. The method of claim 1, further comprising using a second cryptographic
9 algorithm with the decryption key to decrypt the encrypted electronic book.

10 40. The method of claim 1, wherein encrypted electronic books are delivered to home
11 systems individually.

12 41. The method of claim 1, further comprising:
13 providing multiple electronic books to a home system; and
14 supplying the decryption key upon request for a particular electronic book by the
15 home system.

16 42. The method of claim 1, wherein the encrypted electronic book is broadcast to
17 multiple home systems simultaneously.

18 43. The method of claim 42, wherein the encryption key is a transaction symmetric
19 key.

1 44. The method of claim 43, further comprising:
2 encrypting the transaction symmetric key using a first public key corresponding
3 to a first home system;
4 encrypting the transaction symmetric key using second and subsequent public
5 keys corresponding to second and subsequent home systems, respectively;
6 delivering the first through the subsequent encrypted transaction symmetric keys
7 to the multiple home systems;
8 decrypting the delivered first encrypted transaction symmetric key at the first
9 home system using a first private key;
10 decrypting the second and subsequent encrypted transaction symmetric keys at
11 one or more of corresponding ones of the multiple home systems using second and
12 subsequent private keys, respectively; and
13 decrypting the delivered encrypted electronic book at one or more of the multiple
14 home systems using the decrypted transaction symmetric key.

15 45. The method of claim 44, further comprising:
16 assigning one or more of the multiple home systems to one or more predefined
17 groups;
18 generating a group symmetric key for each of the one or more groups of home
19 systems; and
20 distributing the corresponding group symmetric key to each home system in the
21 one or more groups of home systems.

22 46. The method of claim 1, wherein the encrypted electronic book is delivered to a
23 home system, the home system comprising:
24 a library; and
25 a viewer.

1 47. The method of claim 46, wherein security processing is completed in the library.

2 48. The method of claim 46, wherein security processing in completed in the viewer.

3 49. The method of claim 46, further comprising completing security processing
4 between the viewer and the library.

5 50. The method of claim 49, further comprising:
6 receiving the encrypted electronic book at the library;
7 decrypting the received electronic book;
8 storing the decrypted electronic book in a memory;
9 retrieving the stored electronic book;
10 encrypting the retrieved electronic book using a symmetric key;
11 encrypting the symmetric key using a library private key;
12 delivering the encrypted electronic book and the encrypted symmetric key to the
13 viewer;

14 decrypting the encrypted symmetric key using a viewer public key; and
15 decrypting the encrypted electronic book using the decrypted symmetric key.

16 51. The method of claim 50, wherein the symmetric key is randomly generated.

17 52. The method of claim 50, wherein the symmetric key is generated by a key
18 generator process.

19 53. The method of claim 50, wherein the symmetric key is previously defined, further
20 comprising retrieving the previously-defined symmetric key.

1 54. The method of claim 1, further comprising performing integrity checking of the
2 electronic book.

3 55. The method of claim 54, wherein the step of integrity checking, comprises:
4 calculating a first hashing value based on content of the electronic book and a
5 hashing algorithm;
6 associating the first hashing value with the electronic book
7 calculating a second hashing value using the decrypted electronic book and the
8 hashing algorithm;
9 comparing the first and the second hashing values; and
10 storing the decrypted electronic book when the first and the second hashing values
11 match.

12 56. The method of claim 54, wherein a digital signature algorithm is used to identify
13 the sending party.

14 57. The method of claim 1, further comprising verifying an identity of a party sending
15 the electronic book.

16 58. The method of claim 57, wherein the verifying step, comprises:
17 delivering a password with the electronic book;
18 comparing the delivered password with a pre-defined password; and
19 storing the delivered electronic book when the delivered password and the pre-
20 defined password match.

21 59. The method of claim 57, wherein the verifying step comprises decrypting the
22 delivered electronic book using the decryption key.

1 60. The method of claim 57, wherein the verifying step comprises
2 sending a delivery notification message from a sending party to a receiving party
3 receiving the electronic book
4 encrypting a randomly generated message;
5 returning the randomly generated message to the sending party sending the
6 delivery notification message; and
7 decrypting the randomly generated message;
8 re-encrypting the randomly generated message; and
9 returning the re-encrypted randomly generated message to the receiving party with
10 the encrypted electronic book.

11 61. The method of claim 57, wherein the verifying step comprises using an ISO
12 standard X.509 one-way authentication protocol.

13 62. The method of claim 1, further comprising verifying an identity of a first party
14 requesting the electronic book.

15 63. The method of claim 62, wherein the verifying step, comprises:
16 receiving an electronic book request from the first party;
17 generating an authentication string;
18 sending the authentication string to the first party; and
19 returning a response message, wherein the response message, comprises:
20 an identifier that identifies the requested electronic book,
21 a signed authentication string, wherein the signed authentication string is
22 signed using a one-way hash function and wherein the signed authentication string is
23 encrypted, and
24 a first party certification information.

64. The method of claim 1, further comprising:
creating a non-secure metadata header for the electronic book;
creating a secure metadata header for the electronic book, wherein the secure
metadata header includes one or more of an electronic book identifier, the decryption key,
a decryption algorithm, a number of copies of the electronic book that are allowed to be
derived from an original electronic book file, distribution and fair use features and
integrity checking information; and
packaging the non-secure and the secure headers with the electronic book to
create an electronic book distribution file.

65. The method of claim 64, further comprising:
compressing the electronic book distribution file; and
sending the electronic book distribution file to a receiving party.

66. The method of claim 65, wherein the receiving party is an operations center of a
television distribution system.

67. The method of claim 65, wherein the receiving party is an electronic book home
system.

68. The method of claim 65, wherein the receiving party is a library.

69. The method of claim 65, wherein the receiving party is a kiosk.

70. The method of claim 65, wherein the electronic book distribution file is
distributed by a publisher.

1 71. The method of claim 65, wherein the electronic book distribution file is
2 distributed by an operations center.

3 72. The method of claim 65, wherein the electronic book distribution file is
4 distributed by a library.

5 73. The method of claim 65, wherein the electronic book distribution file is
6 distributed by an electronic book home system.

7 74. The method of claim 65, wherein the electronic book distribution file is
8 distributed at a kiosk.

9 75. The method of claim 65, wherein the electronic book distribution file is delivered
10 from a first viewer to a second viewer.

11 76. The method of claim 65, wherein the electronic book distribution file is
12 distributed over an Internet using a secure socket layer protected communication link.

13 77. The method of claim 76, wherein the receiving party sends an electronic book
14 request message to request the electronic book, the request message including an Internet
15 Protocol address of the receiving party.

16 78. The method of claim 77, wherein the request message includes a login and
17 password sequence.

18 79. The method of claim 77, further comprising:
19 sending a certificate to the receiving party, the certificate including information
20 identifying a sending party and a sending party public key;

1 verifying the certificate by comparing the information included in the certificate
2 to expected values for the information;
3 sending an algorithms supported message to the sending party;
4 returning a selected algorithm to the receiving party;
5 generating a transaction symmetric key;
6 encrypting the transaction symmetric key using the sending party public key and
7 the selected algorithm;
8 sending the encrypted transaction symmetric key to the sending party;
9 decrypting the encrypted transaction symmetric key using a sending party private
10 key; and
11 using the transaction symmetric key to encrypt and to decrypt a transaction
12 between the sending party and the receiving party.

13 80. The method of claim 76, wherein a sending party sends an electronic book
14 distribution message to the receiving party, the distribution message including Internet
15 Protocol address of the sending party.

16 81. The method of claim 80, wherein the distribution message further comprises a
17 login and password sequence.

18 82. The method of claim 81, further comprising:
19 sending a certificate to the sending party, the certificate including information
20 identifying a sending party and a receiving party public key;
21 verifying the certificate by comparing the information included in the certificate
22 to expected values for the information;
23 sending an algorithms supported message to the receiving party;
24 returning a selected algorithm to the sending party;
25 generating a transaction symmetric key;

1 encrypting the transaction symmetric key using the receiving party public key and
2 the selected algorithm;
3 sending the encrypted transaction symmetric key to the receiving party;
4 decrypting the encrypted transaction symmetric key using a receiving party private
5 key; and
6 using the transaction symmetric key to encrypt and to decrypt a transaction
7 between the sending party and the receiving party.

8 83. The method of claim 1, wherein the electronic book is delivered to a receiving
9 party by a sending party, the method further comprising verifying that the receiving party
10 received the electronic book.

11 84. The method of claim 83, wherein the verifying step, comprises:
12 generating a reply message;
13 encrypting the reply message using a private key of the receiving party;
14 encrypting the encrypted reply message using a public key of the sending party;
15 sending the doubly encrypted reply message to the sending party; and
16 decrypting the doubly encrypted reply message using a private key of the sending
17 party and a public key of the receiving party.

18 85. The method of claim 83, wherein the verifying step comprises using an ISO
19 standard X.509 two-way authentication protocol framework.

20 86. The method of claim 1, wherein encryption key information is supplied between
21 a sending party and a receiving party using a telecommunications network.

22 87. The method of claim 86, wherein the telecommunications network comprises one
23 or more of a television delivery system, a wired telephone network, a wireless telephone

1 network, a personal communications network (PCS), an Internet, an intranet, a local area
2 network, a radio communications network, and an optical fiber network.

3 88. The method of claim 1, wherein encryption key information is supplied between
4 a sending party and a receiving party using a portable memory storage device.

5 89. The method of claim 88, wherein the portable memory storage device includes
6 one or more of a PCMCIA card, a CD ROM, a memory stick, and a smart card.

7 90. The method of claim 89, wherein the encryption key includes a valid time period
8 of use.

9 91. The method of claim 89, wherein the portable memory storage device is updated
10 remotely using a telecommunications network.

11 92. The method of claim 1, further comprising:
12 receiving the encrypted electronic book at a receiving party; and
13 storing the electronic book in an encrypted format in a memory storage device.

14 93. The method of claim 92, wherein the encrypted storage is performed at a driver
15 level, comprising:
16 encrypting the electronic book using a memory storage device driver level; and
17 storing the encrypted electronic book at the memory storage device.

18 94. The method of claim 93, wherein the electronic book is encrypted using a
19 symmetric key.

1 95. The method of claim 92, wherein the encrypted storage is performed at a file
2 level, further comprising:

3 encrypting the electronic book using a unique symmetric key;
4 storing the encrypted electronic book in the memory storage device; and
5 storing the symmetric key, wherein the symmetric key is stored in a memory
6 location apart from a memory location for the electronic book.

7 96. The method of claim 92, further comprising:

8 computing a first hashing value, using a one-way hashing algorithm and the
9 electronic book, prior to encrypting the electronic book and storing the encrypted
10 electronic book in the memory storage device;

11 storing the first hashing value;
12 retrieving the encrypted electronic book and the first hashing value;
13 decrypting the retrieved encrypted electronic book;
14 computing a second hashing value using the retrieved decrypted electronic book
15 and the one-way hashing algorithm; and

16 comparing the first and the second hashing values, wherein when the first and the
17 second hashing values coincide, an integrity of the stored encrypted electronic book is
18 assured.

19 97. An electronic book viewer for receiving an electronic book from a sending party,
20 and for storing and displaying the electronic book, comprising:

21 a receiver that receives encrypted electronic books and encryption information;
22 a memory coupled to the receiver that stores the encrypted electronic books and
23 the encryption information;

24 a processor coupled to the memory that processes the encryption information
25 using an encryption/decryption algorithm, wherein the processor comprises:

26 a key generator that generates encryption and decryption keys; and

1 a transmitter coupled to the processor that sends encryption information to the
2 sending party, wherein the encryption information includes information that allows
3 encryption and decryption of the electronic book and encryption and decryption of
4 encryption and decryption keys.

5 98. The electronic book viewer of claim 97, wherein the encryption keys and the
6 decryption keys are symmetric keys.

7 99. The electronic book viewer of claim 98, wherein the symmetric keys are
8 generated randomly.

9 100. The electronic book viewer of claim 98, wherein the memory stores the symmetric
10 keys, and wherein the processor retrieves a stored symmetric key from the memory.

11 101. The electronic book viewer of claim 98, wherein the receiver receives a
12 transaction symmetric key from a certificate authority, and the memory stores the
13 transaction symmetric key.

14 102. The electronic book viewer of claim 101, wherein the processor generates a
15 transaction symmetric key request, the transmitter sends the request to the certificate
16 authority and the receiver receives an encrypted transaction symmetric key, and wherein
17 the processor uses the encrypted transaction symmetric key to decrypt the encrypted
18 received electronic book.

19 103. The electronic book viewer of claim 98, wherein the symmetric key is encrypted
20 with a private key and a private encryption algorithm and wherein the processor decrypts
21 the encrypted symmetric key using a public key and a public key decryption algorithm.

104. The electronic book viewer of claim 98, wherein the processor further comprises a shared key negotiation algorithm, wherein the symmetric key is a shared transaction symmetric key, and wherein the processor negotiates with the sending party to generate the shared transaction symmetric key.

105. The electronic book viewer of claim 97, wherein the processor further comprises a first seed key generation algorithm and a second seed key generation algorithm, the processor using the first seed key generation algorithm to generate an encryption key and using the second seed key generation algorithm to generate a decryption key.

106. The electronic book viewer of claim 97, wherein an encryption key is a public key and a decryption key is a private key.

107. The electronic book viewer of claim 97, wherein the encryption key is a private key and the decryption key is a public key.

108. The electronic book viewer of claim 97, wherein the receiver receives a decryption key with the electronic book.

109. The electronic book viewer of claim 108, wherein the decryption key is encrypted before shipment to the electronic book viewer.

110. The electronic book viewer of claim 97, wherein the electronic book is encrypted using one of DES, PKZIP and BLOWFISH encryption algorithms.

111. The electronic book viewer of claim 97, wherein the encrypted electronic books are broadcast to the electronic book viewer.

1 112. The electronic book viewer of claim 111, wherein the electronic book is encrypted
2 using a first public key system corresponding to the electronic book viewer.

3 113. The electronic book viewer of claim 97, wherein the electronic book viewer is
4 assigned to one or more predefined groups of electronic book viewers.

5 114. The electronic book viewer of claim 97, further comprising a library unit coupled
6 to the electronic book viewer, wherein the library unit completes security processing.

7 115. The electronic book viewer of claim 97, wherein the processor includes an
8 integrity checking algorithm.

9 116. The electronic book viewer of claim 97, wherein the processor includes a
10 verification algorithm that verifies an identity of the sending party.

11 117. The electronic book of claim 97, wherein the processor includes an authentication
12 algorithm.

13 118. The electronic book of claim 97, wherein the sending party is a book publisher.

14 119. The electronic book viewer of claim 97, wherein the sending party is an
15 operations center of a cable television delivery system.

16 120. The electronic book viewer of claim 97, wherein the sending party sends
17 electronic books using an Internet web site.

18 121. The electronic book viewer of claim 97, wherein the sending party is a kiosk.

1 122. The electronic book viewer of claim 97, wherein the sending party is another
2 electronic book viewer.

3 123. The electronic book viewer of claim 97, wherein the electronic book viewer
4 receives encrypted electronic books and encryption information using a
5 telecommunications network.

6 124. The electronic book viewer of claim 123, wherein the telecommunications
7 network includes one or more of a television delivery system, a wired telephone system,
8 a wireless telephone network, a personal communications network, a wired Internet
9 system, a wireless Internet system, an intranet, a local area network, a radio
10 communications network, and an optical fiber network.

11 125. The electronic book viewer of claim 97, further comprising a data entry port,
12 wherein the electronic book viewer receives encryption key information using the data
13 entry port and a portable memory storage device.

14 126. The electronic book viewer of claim 125, wherein the portable memory storage
15 device includes one or more of a PCMCIA card, a CD ROM, a smart card and a memory
16 stick.

17 127. The electronic book viewer of claim 126, wherein the encryption key includes a
18 valid time period of use.

19 128. The electronic book viewer of claim 126, wherein the encryption key includes a
20 valid time period of use.

1 129. The electronic book viewer of claim 125, wherein the portable memory storage
2 device is updated remotely using a telecommunications network.

3 130. A system for encrypting an electronic book for delivery from a first party to a
4 second party, comprising:

5 a first interface that receives and transmits electronic books and encryption
6 information;

7 a first memory coupled to the first interface that stores the electronic books and
8 the encryption information;

9 a first processor coupled to the first interface and the first memory that processes
10 the encryption information and encrypts and decrypts the electronic books;

11 a second interface that receives electronic books transmitted from the first party,
12 and that receives and transmits encryption information;

13 a second memory coupled to the second interface that stores the received
14 electronic books and the encryption information; and

15 a second processor coupled to the second interface and the second memory that
16 processes the encryption information and that decrypts the received electronic books.

17 131. The system of claim 130, wherein the first and the second parties are coupled to
18 a communications network, and wherein the encryption information and the electronic
19 books are transmitted and received using the communications network.

20 132. The system of claim 131, wherein the communications network includes one or
21 more of a television delivery system, a wired telephone system, a wireless telephone
22 network, a personal communications network, a wired Internet system, a wireless Internet
23 system, an intranet, a local area network, a radio communications network, and an optical
24 fiber network.

1 133. The system of claim 130, wherein the encryption information includes an
2 encryption key and a decryption key.

3 134. The system of claim 133, wherein the encryption key and the decryption keys
4 comprise a symmetric key.

5 135. The system of claim 134, wherein the first processor comprises a first key
6 generator, the first key generator generating the symmetric key.

7 136. The system of claim 135, wherein the first key generator generates the symmetric
8 key randomly.

9 137. The system of claim 134, wherein the second processor comprises a second key
10 generator, the second key generator generating the symmetric key.

11 138. The system of claim 137, wherein the second key generator generates the
12 symmetric key randomly.

13 139. The system of claim 134, wherein the first processor and the second processor
14 retrieve the symmetric key from the first and the second memories, respectively.

15 140. The system of claim 134, wherein the symmetric key is a transaction symmetric
16 key, the transaction symmetric key supplied by a third party.

17 141. The system of claim 140, wherein the third party is a certificate authority.

18 142. The system of claim 141, wherein the certificate authority issues the transaction
19 symmetric key encrypted.

1 143. The system of claim 142, wherein the transaction symmetric key is encrypted by
2 the certificate authority using a first party symmetric key.

3 144. A method for secure distribution of electronic books, comprising:
4 receiving an electronic book;
5 obtaining an encryption key;
6 processing the electronic book using the encryption key and an encryption
7 algorithm;
8 sending the encrypted electronic book to a recipient;
9 obtaining a decryption key; and
10 decrypting the encrypted electronic book using the decryption key and a
11 decryption algorithm.

12 145. The method of claim 144, wherein the encrypted electronic book is broadcast to
13 multiple home systems simultaneously.

14 146. The method of claim 145, wherein the encryption key is a transaction symmetric
15 key.

16 147. The method of claim 146, further comprising:
17 encrypting the transaction symmetric key using a first public key corresponding
18 to a first home system;
19 encrypting the transaction symmetric key using second and subsequent public
20 keys corresponding to second and subsequent home systems, respectively;
21 delivering the first through the subsequent encrypted transaction symmetric keys
22 to the multiple home systems;

1 decrypting the delivered first encrypted transaction symmetric key at the first
2 home system using a first private key;

3 decrypting the second and subsequent encrypted transaction symmetric keys at
4 one or more of corresponding ones of the multiple home systems using second and
5 subsequent private keys, respectively; and

6 decrypting the delivered encrypted electronic book at one or more of the multiple
7 home systems using the decrypted transaction symmetric key.

8 148. The method of claim 147, further comprising:

9 assigning one or more of the multiple home systems to one or more predefined
10 groups;

11 generating a group symmetric key for each of the one or more groups of home
12 systems; and

13 distributing the corresponding group symmetric key to each home system in the
14 one or more groups of home systems.

15 149. The method of claim 144, further comprising storing the electronic book in
16 memory as an encrypted file.

17 150. The method of claim 144, wherein the encrypted electronic book is sent by a
18 publisher and the recipient is an operations center of an electronic book distribution
19 system.

20 151. The method of claim 144, wherein the encrypted electronic book is sent by an
21 operations center and the recipient is a home system.

22 152. The method of claim 144, wherein the encrypted electronic book is sent by a
23 lending facility and the recipient is a home system.

1 153. The method of claim 144, wherein the encrypted electronic book is sent by a
2 home system library and the recipient is a home system viewer.

3 154. The method of claim 144, wherein the encrypted electronic book is sent by a first
4 home system viewer and the recipient is a second home system viewer.

5 155. The method of claim 144, further comprising creating a protected metadata header
6 related to the electronic book, wherein the protected metadata header comprises an
7 electronic book identifier, a metadata format identifier, the decryption key, and a
8 decryption algorithm.

9 156. The method of claim 155, wherein the protected metadata header is provided with
10 the encrypted electronic book.

11 157. The method of claim 155, wherein the protected metadata header is provided
12 separate from the encrypted electronic book.

13 158. The method of claim 155, wherein the protected metadata header further
14 comprises a number of allowed copies of the encrypted electronic book, distribution
15 features supported for the electronic book, fair use features and integrity checking
16 information.

17 159. The method of claim 158, wherein the fair use features comprise using the
18 electronic book for a specified time.

19 160. The method of claim 159, wherein the fair use features comprise a print enable
20 function.

1 161. The method of claim 160, wherein the print enable function enables a specified
2 number of copies of the electronic book to be printed.

3 162. The method of claim 158, wherein the distribution features comprise a loan enable
4 feature, the loan enable feature allowing a sending party to send the electronic book to
5 one or more recipients.

6 163. The method of claim 144, further comprising compressing the encrypted
7 electronic book before sending to the recipient.

8 164. The method of claim 144, further comprising authenticating an identity of the
9 recipient.

10 165. The method of claim 164, wherein the authenticating step comprises using a
11 digital signature algorithm.

12 166. The method of claim 164, wherein the authenticating step comprises using a
13 password.

14 167. The method of claim 144, wherein the step of sending the encrypted electronic
15 book comprises sending the encrypted electronic book to a remote location, wherein the
16 recipient retrieves the encrypted electronic book from the remote location.

17 168. The method of claim 167, wherein the remote location is an Internet website.

18 169. The method of claim 167, wherein the remote location is a computer, and wherein
19 the recipient is coupled to the computer.

1 170. The method of claim 169, wherein the recipient and the computer are coupled by
2 a communications network.

3 171. The method of claim 169, wherein the communications network is an infra red
4 network.

5 172. The method of claim 169, wherein the communications network is a radio
6 frequency network.

7 173. The method of claim 167, wherein the sending party removes the encrypted
8 electronic book from the remote location after a specified time.

9 174. The method of claim 144, wherein the recipient is a home system, further
10 comprising:

11 registering the home system with the sending party;
12 assigning the home party an electronic book deposit location; and
13 sending electronic books for the home system to the deposit location.

14 175. The method of claim 174, further comprising sending decryption information to
15 the deposit location.

16 176. The method of claim 174, wherein the sending party obtains information from the
17 home system during the registering step, and wherein the information includes an internal
18 serial number of the home system.

19 177. The method of claim 144, further comprising:
20 generating a reply message upon receipt of the encrypted electronic book; and

1 returning the reply message to the sending party, the reply message indicating
2 receipt of the encrypted electronic book.

3 178. The method of claim 144, further comprising:
4 generating a reply message upon decrypting the encrypted electronic book; and
5 returning the reply message to the sending party.

6 179. The method of claim 144, wherein the recipient is a public viewer.

7 180. The method of claim 144, further comprising sending a data header with the
8 encrypted electronic book, wherein the data header comprises a time duration for
9 retention of the electronic book by the recipient.

10 181. The method of claim 144, wherein a first part of the electronic book is encrypted
11 and a second part of the electronic book is not encrypted.

12 182. The method of claim 144, further comprising applying a copyright notice to the
13 electronic book.

14 183. The method of claim 144, wherein stenographic information is embedded in the
15 electronic book.

16 184. The method of claim 183, wherein the stenographic information identifies a valid
17 recipient viewer.

18 185. The method of claim 184, wherein a viewer displays only electronic books for
19 which the stenographic information matches the displaying viewer.

1 186. The method of claim 144, wherein the encryption and the decryption algorithms
2 are updated using a software download over a distribution network.

3 187. The method of claim 144, wherein the encryption and the decryption algorithms
4 are updated using physical media.

5 188. The method of claim 187, wherein the physical media comprises one of a
6 PCMCIA card, a smart card, a memory stick and a memory device.

7 189. The method of claim 144, wherein the electronic book comprises one or more
8 pages and wherein a viewer decrypts the electronic book page by page, each page of the
9 one or more pages of the electronic book being decrypted just before viewing.